REVISTA
JURÍDICA
ISSN 1390-3071

Presupuestos criminológicos para el abordaje de la ciberdelincuencia patrimonial contra personas naturales en Cuba

Criminological assumptions for addressing cybercrime against individuals in Cuba

Camila María González Font[1]

[1] Universidad de La Habana, Cuba. *camila.mgonzalez@lex.uh.cu*

PARA CITAR ESTE ARTÍCULO
Gómez Font, C. M. Presupuestos criminológicos para el abordaje de la ciberdelincuencia patrimonial contra personas naturales en Cuba. *Revista Jurídica*, (36).

DOI
https://doi.org/10.23878/rj.i36.608

CORRESPONDENCIA
camila.mgonzalez@lex.uh.cu

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Av. Carlos Julio Arosemena, Km 1,5. Guayaquil, Ecuador
Teléfono: +593 4 380 4600
Correo electrónico: revista.alternativas@cu.ucsg.edu.ec
Web: www.ucsg.edu.ec

Presupuestos criminológicos para el abordaje de la ciberdelincuencia patrimonial contra personas naturales en Cuba

Criminological assumptions for addressing cybercrime

Camila María González Font[1]

[1] Universidad de La Habana, Cuba. *camila.mgonzalez@lex.uh.cu*

RESUMEN

Con la apertura de Cuba al internet, la nación y los usuarios de las redes, se han enfrentado con una de las más nocivas prácticas del uso de las TIC, en un contexto complejo para su prevención y enfrentamiento. Específicamente la ciberdelincuencia patrimonial, es una de las expresiones más comunes de ciberdelincuencia en la Cuba de hoy. Los comisores de estos hechos se aprovechan de las características el ciberespacio, el desconocimiento, la ingenuidad y la baja percepción del peligro en los usuarios de las redes, las vulnerabilidades y brechas de seguridad de los sistemas informáticos y las fallas en el control social formal, y valiéndose de sus conocimientos informáticos, cometen actos en detrimento del patrimonio de las personas naturales generando significativos daños en la economía de estas y debilitando la confianza en el ecosistema digital, al que Cuba se inserta. El presente artículo científico persigue como objetivo, determinar y analizar los presupuestos criminológicos para el abordaje de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba en vistas a obtener los basamentos fundamentales para el diseño de estrategias preventivas de dicho fenómeno.

PALABRAS CLAVE: presupuestos criminológicos, abordaje, ciberdelincuencia patrimonial, estrategias preventivas.

ABSTRACT

With Cuba's opening to the internet, the nation and its users have faced one of the most harmful practices associated with the use of ICTs, in a complex context for its prevention and combating. Specifically, cybercrime targeting assets is one of the most common forms of cybercrime in Cuba today. Those who commit these acts take advantage of the characteristics of cyberspace, the lack of knowledge, naiveté, and low perception of danger among network users, the vulnerabilities and security gaps in computer systems, and the shortcomings in formal social control. Leveraging their computer skills, they commit acts that harm the assets of individuals, causing significant damage to their finances and weakening trust in the digital ecosystem to which Cuba belongs. The objective of this scientific article is to determine and analyze the criminological assumptions for addressing cybercrime affecting individuals in Cuba, with a view to obtaining the fundamental bases for the design of preventive strategies for this phenomenon.

KEYWORDS: criminological budgets, approach, cybercrime against property, preventive strategies.

RECIBIDO: 04/12/2025
ACEPTADO: 11/12/2025

CORRESPONDENCIA:
camila.mgonzalez@lex.uh.cu

Introducción

Es la aparición de las Tecnologías de la Información y las Comunicaciones (TIC) pero sobre todo su masificación, el elemento que mejor define la nueva era que se vive. Si algo ha revolucionado la sociedad es Internet, gran invento del siglo XX y símbolo de la época actual. Internet ha facilitado las relaciones sociales, y en general toda comunicación e intercambio de información.

Las estadísticas arrojan un imparable y progresivo crecimiento de las personas que acceden habitualmente a Internet año tras año. Esto sin duda prueba su consolidación como elemento comunicativo, comercial o de ocio[1]. La evolución hacia la sociedad de la información ha supuesto una transformación profunda de las relaciones sociales, y uno de los efectos de dicho proceso ha sido la transformación de la delincuencia[2].

Con la apertura de Cuba al internet debido a la informatización de la sociedad, el incremento del uso de las redes sociales, la tecnología, el uso de la telefonía celular, el acceso de mayor cantidad de personas al comercio electrónico y las transacciones comerciales, los usuarios de las redes, se han enfrentado con una de las más nocivas prácticas del uso de las Tecnologías de la Información y las Comunicaciones, los ciberdelitos.

Desde la apertura de Cuba al internet, con un auge significativo en el período de la Covid-19, hubo personas que, aprovechando sus conocimientos informáticos advirtieron brechas favorables y comenzaron a realizar actos con el objetivo de enriquecer su patrimonio personal en detrimento del ajeno, empleando para dichos actos delictivos las TIC. Las estafas informáticas y el robo con fuerza en las cosas han cobrado especial auge, siendo numerosas las víctimas y significativos los daños patrimoniales causados a la economía de estas.

La ciberdelincuencia patrimonial contra las personas naturales muestra, en Cuba, matices particulares que deben ser analizados y tenidos en cuenta para proyectar correcta y eficazmente una estrategia para su prevención. Es por ello que este estudio se propone ofrecer una propuesta sustentada en elementos teóricos, jurídicos y criminológicos que permita abordar el fenómeno de la ciberdelincuencia patrimonial que afecta a personas naturales, contextualizada a la realidad cubana, y que tribute a la prevención del mismo.

Acercamiento jurídico, doctrinal y criminológico a la ciberdelincuencia

El crecimiento de la sociedad de la información viene acompañado de nuevas e importantes amenazas producto de la aparición de nuevas conductas delictivas y de una mayor facilidad para cometer delitos convencionales, surgiendo así la ciberdelincuencia. Esta

---

1 Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución. El Convenio de Budapest", Revista Electrónica de Derecho de La Universidad de la Rioja (REDUR), Número 8, 2010, p.171. Disponible en: https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

2 Tamarit Sumalla, Josep, "Ciberdelincuencia y victimización", Revista de Internet Derecho y Política, Número 22, 2016. Disponible en: http://journals.uoc.edu/index.php/idp/article/view/n22-tamarit/n22-tamarit-pdf-es>http://dx.doi.org/10.7238/idp.v0i22.2991>

otra cara de la moneda deja al descubierto la aparición de un nuevo factor criminógeno. El mundo vive una época de digitalización, hasta cierto punto peligrosa, todos los centros operacionales funcionan y son dirigidos por medio de las tecnologías: servicios esenciales tales como el suministro de agua y electricidad, el funcionamiento de automóviles, el control de tráfico, los ascensores, el aire acondicionado, los teléfonos, las fábricas, las operaciones comerciales dependen del correcto funcionamiento de las TIC[3].

La tendencia indica que cada vez empleamos más tiempo de nuestro día en navegar por la red y, en consecuencia, cada vez, trasladamos más parcelas de nuestra vida al mundo virtual. Esto se traduce en que cada vez introducimos más valores personales en el ciberespacio, lo que permite a los ciberdelincuentes tener disponibles cada vez más bienes jurídicos para su lesión o puesta en peligro[4]. Este desplazamiento de las oportunidades al ciberespacio fruto del mayor tiempo y más actividades realizadas en internet se traduce necesariamente en un aumento de los ciberdelitos[5].

La cuestión más preocupante es la vertiginosa velocidad con la que evolucionan las nuevas tecnologías y el consiguiente y constante cambio y desarrollo, también extremadamente rápido, de las conductas delictivas vinculadas a las mismas. Ello hace que merezca la pena reflexionar antes de abordar el fenómeno en los aspectos jurídicos y doctrinales en torno a la ciberdelincuencia como fenómeno.

Con respecto a la conceptualización de los ciberdelitos es necesario recalcar que hay múltiples definiciones, sin embargo, el aspecto esencial de todas y cada una de ellas se reduce a la cuestión de si con la definición se está adoptando una concepción amplia o restringida de la cibercriminalidad, dando cobertura en la categoría a todos, o tan solo, a algunos de los comportamientos criminales realizados en el ciberespacio.

La ciberdelincuencia en sentido amplio concibe como ciberdelito a aquel comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo al ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet. Por el contrario, la ciberdelincuencia en sentido res-

[3] Vid, División de Aplicaciones TIC y Ciberseguridad. Departamento de Políticas y Estrategias. Sector de Desarrollo de las Telecomunicaciones de la UIT, "El ciberdelito: Guía para los países en desarrollo", Proyecto de abril de 2009, p.11. Disponible en: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

[4] Gorostidi, Jon López, "Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia", Revista chilena de Derecho y Tecnología, Volumen 11, Número 1, Santiago de Chile, junio 2022, p.122. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842022000100121&lng=es&nrm=iso.

[5] Miró Llinares, Fernando Crimen, cibercrimen y COVID-19, "Desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", Revista de Internet, derecho y política, Número 32, 2021, p.4. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7962061

tringido admite como ciberdelito únicamente al comportamiento delictivo realizado en el ciberespacio, cuya esencia de injusto no podría haberse dado de ninguna otra manera fuera de él.

De ahí que en la doctrina se distinga entre ciberdelitos propios, "propiamente informáticos" o ciberdelitos en sentido restringido o estricto, y los ciberdelitos impropios, que son los "delitos configurados a través de internet" o ciberdelitos en sentido amplio. Categorizando como propios a aquellos que se pueden cometer sólo por medio de las TIC, y como impropios a aquellos delitos clásicos en los que las TIC son sólo un nuevo medio comisivo[6]. En el primer grupo quedan englobadas las conductas como el sabotaje informático, la piratería informática, el hackeo, el crackeo, mientras que en el segundo grupo se encuentran la falsificación de documentos electrónico, falsificación y clonación de tarjetas de crédito, robo de identidad, estafas informáticas, fraudes electrónicos y pornografía infantil.

En este sentido refiere Miró LLinares[7] que en los últimos tiempos se ha venido sustituyendo, aunque no por todos, la denominación de "Delitos Informáticos"[8] por la de "Cibercrimen" y "Cibercriminalidad" en referencia esta vez al término anglosajón cybercrime. Destaca el autor que en la raíz de este cambio de denominación está la evolución de ser la información del sistema informático el centro del riesgo, a serlo las redes telemáticas, a las que los sistemas empezaron a estar conectados y los intereses personales y sociales que se ponen en juego en las mismas. Resaltando que, a la primera generación de la cibercriminalidad, donde lo característico era el uso de ordenadores para la comisión de delitos, le ha sucedido una segunda época en la que la característica central es que el delito se comete a través de Internet, y una tercera en la que los delitos están absolutamente determinados por el uso de Internet y las TIC. Y que todo ello ha llevado a la utilización de un término, el de "cibercrimen", que logra englobar todas las tipologías de comportamientos pueden integrarla, y además alcanza mejor que otros el propósito esencial del concepto que es el Internet y las TIC como medio de comisión delictiva.

Se coincide con el autor citado, no obstante, la distinción que aun pueda existir en la doctrina en lo concerniente a la terminología o a la conceptualización, lo cierto es que la criminalidad informática, ciberdelincuencia o delincuencia informática como categoría

6 Vid, Gil, Leandro (Coord.), Cibercrimen y Delitos Informáticos. Guía de Estudio, año 2021, p.46. Disponible en: https://www.mseg.gba.gov.ar/areas/Vucetich/MANUALES%20DE%20MATERIAS%202022/MANUAL%20Cibercrimen%20y%20delitos%20inform%C3%A1ticos.pdf

7 Miró Llinares, Fernando, El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Madrid, Ediciones Jurídicas y Sociales. S.A, Marcial Pons, 2012, p.37.

8 NA: En puridad no puede hablarse de un delito informático, sino de una pluralidad de delitos en los que nos encontramos, como única nota común, su vinculación de alguna manera con los ordenadores, pero ni el bien jurídico agredido es siempre de la misma naturaleza ni la forma de comisión del hecho delictivo o merecedor de serlo presenta siempre características semejantes. Vid, Barrio Andrés, Moisé, "La ciberdelincuencia en el Derecho Español", Revista de las Cortes Generales, Número 83, 2011, p.277.

general, amplia y de base criminológica hace referencia al ámbito de riesgo que sirve de base común al comportamiento que utiliza la red para la realización de comportamientos constitutivo de delito.

La palabra delincuencia, según la Real academia de la Lengua española, es el conjunto de delitos, ya en general o ya referidos a un país, época o especialidad en ellos. Ciberdelincuencia entonces es la combinación del prefijo Ciber- que proviene del inglés Cyber que indica redes informáticas con el término delincuencia. Es por ello que la diferencia entre delincuencia y ciberdelincuencia será el espacio o medio donde se desarrolla el delito. Se refiere el término ciberdelincuencia, por tanto, al fenómeno de la criminalidad en el ciberespacio.

La ciberdelincuencia como categoría criminológica, engloba no solo aquellos delitos que atacan la informática, su integridad, sistema y datos, sino aquellos que, empleando medios informáticos, dañan los bienes jurídicos tradicionalmente protegidos como el patrimonio, la indemnidad sexual, el honor, entre otros. Se denomina, entonces, ciberdelincuente a quien opera de manera ilícita y ocultándose en las redes, a través de dispositivos electrónicos o de telecomunicaciones, en el espacio virtual o el ciberespacio, a quien le será atribuida responsabilidad penal conforme a lo previsto por el delito cometido por este.

A los efectos del desarrollo de este trabajo se considerará como ciberdelito a aquella acción típica y antijurídica que es cometida a través de las TIC, atentando a la disponibilidad, integridad y confidencialidad de los sistemas informáticos, de las redes, de los datos y derechos de terceros, o haciendo un uso fraudulento de ellos. El ciberdelito comprende todas aquellas conductas en las que las TIC son el objetivo o el medio de ejecución del delito, aunque afecten bienes jurídicos diversos. Con ello se advierte que el concepto de ciberdelito abarca los delitos cometidos a través de la informática, los delitos cometidos contra la informática y aquellos delitos cometidos contra y a través de los sistemas informáticos.

Con respecto al bien jurídico protegido se puede afirmar que los ciberdelitos no sólo dañan en su comisión bienes jurídicos propiamente informáticos, sino que su objeto de protección coincide con el de los tipos tradicionales que están siendo adaptados a las nuevas tecnologías, a la vez que pone en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos, de las redes de transmisión de datos y la integridad de los sistemas informáticos, telecomunicaciones, las tecnologías de la información y la comunicación y sus servicios. La gravedad de este quebrantamiento de confianza radica, precisamente, en la dependencia de la sociedad actual respecto de las TIC para el desarrollo personal, económico y social de los individuos.

Una de las clasificaciones en la doctrina es la que clasifica los ciberdelitos en delitos cibereconómicos o patrimoniales que son los que afectan al patrimonio de sus víctimas, los delitos ciberintrusivos que son los que dañan la esfera más personal de los ciudadanos, ya que son los relativos a bienes jurídicos personalísimos como la intimidad, la libertad, la libertad sexual o el honor, y los delitos de ciberterrorismo que afectan a la paz pública[9].

[9] López Gorostidi, Jon. op.cit; p. 128.

Frente a la primera visión que ofrecía la criminalidad informática de ser una modalidad de delincuencia muy específica, relacionada con concretas tecnologías y con reducidos usos de la misma, hoy la única visión posible, por funcional, sobre la cibercriminalidad es la de una delincuencia amplia, variada y cambiante que ni puede asociarse a una concreta tecnología o a un específico grupo de sujetos, ni limitarse a un concreto sector de la actividad social[10]. A continuación, se hará referencia a las características de los ciberdelitos, que constituyen sus principales puntos de divergencia con respecto a la delincuencia convencional[11].

1. Anonimato: dado por el desconocimiento de la identidad del delincuente. La identidad real del delincuente puede quedar oculta, o bien la conexión desde la cual realiza la acción delictiva. Tener conocimientos en la materia y habilidades necesarias permite al ciberdelincuente, además de cometer el hecho, poder encubrirlo. El anonimato conlleva a su vez una difícil persecución del ciberdelito, pues, al desconocer en muchas ocasiones quién es el autor real o desde qué red ha cometido el delito, no es posible condenar el hecho, quedando impune.
2. Inexistencia de barreras geográficas: internet elimina la exigencia de proximidad entre agresor y víctima para la existencia de un delito. El ataque que se pude hacer desde cualquier parte del mundo. En el ciberespacio, los ofensores con inclinaciones criminales pueden radicar en cualquier Estado y pueden actuar sobre víctimas de otros distintos, reduciéndose las barreras que el espacio suele imponer para ello. No se encuentran fronteras geográficas que impidan que la comunicación se mantenga a distancia, viajando la información y el contenido de un país a otro. Las tecnologías permiten la comunicación a distancia a través de las redes. En este sentido, el ciberdelincuente puede encontrarse físicamente alejado de la víctima[12], lo que conlleva a que la conducta antijurídica puede realizarse en un determinado país, pero el resultado puede producirse en otro. Por tanto, el factor geográfico que se ve eliminado o reducido gracias a la existencia de los medios de comunicación telemáticos y sobre todo de Internet, lo que conlleva a que el ciberdelito adquiera un carácter transnacional en ocasiones, que deriva en la intervención de varias jurisdicciones, legislaciones, organizaciones de control e investigación.

---

10 Miró Llinares, Fernando. El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, op.cit; p.28

11 Vid, Cordero Ruiz, Nuria Fernanda, La ciberdelincuencia, Máster Universitario en Acceso a la Profesión de Abogado Universidad de Alcalá, 2021, pp.12-13. Disponible en: https://ebuah.uah.es/dspace/handle/10017/49563

12 NA: Inclusive el ciberdelincuente puede estar en otro país, siendo esto muy usual y conveniente para el ciberdelincuente, dado que varios Estados tienen una escasa o nula regulación sobre esta materia, así como una falta de cooperación judicial internacional, convirtiéndose estos estados en "paraísos cibernéticos", que son aquellos lugares donde es más fácil la comisión de los ciberdelitos.

3. Instantáneos: los ciberdelitos se cometen con gran celeridad e ipso facto. El perfeccionamiento del delito se da en el mismo momento en el que el delincuente lleva a cabo la acción. Se emplea poco tiempo en su comisión y el delito se consuma en cuestión de segundos.
4. Masivos: la masividad como característica de las TIC se ve reflejada en los ciberdelitos, dado que estas permiten la difusión masiva de contenidos. Además, la expansión del ámbito comunicativo al que puede acceder un agresor motivado, que supone el ciberespacio, conlleva una multiplicación de la potencialidad lesiva de una conducta por comparación con lo que ocurre en el espacio físico.
5. Pluriofensivos: pueden afectar a más de un bien jurídico protegido a la vez. Se vulnera el bien jurídico propiamente informático, a la vez que lesiona o pone en peligro otros bienes jurídicos tradicionales, como la intimidad, indemnidad sexual, el honor, el patrimonio, la fe pública, el orden público[13].

Son difíciles de demostrar, debido a los obstáculos que se presentan en la investigación de éstos, por su carácter extremadamente técnico y sofisticado

Circunstancias y oportunidades que propician la ciberdelincuencia

La red es un lugar criminógeno, toda vez que, por sus mismas condiciones, genera delincuencia. Es un espacio propicio que atrae al delincuente a cometer su delito, en el que existen menores riesgos y abundan distintos objetivos vulnerables. La identificación de los factores de riesgo en el ciberespacio plantea muchos problemas. El anonimato de los usuarios, el escaso control social ejercido sobre las redes sociales, las características espacio-temporales del mundo virtual, la multiplicación de las interacciones y el alcance de los actos[14].

Las TIC, en general, e Internet como red global, en particular, han supuesto la creación de un lugar de comunicación social transnacional, universal y en permanente evolución tecnológica, que ha sido denominado Ciberespacio, que deviene un nuevo ámbito de oportunidad delictiva, un contexto de riesgo criminal distinto al espacio nacional físico tradicional[15].

13 Vid, Mayer Lux, Laura, "El bien jurídico protegido en los delitos informáticos", Revista chilena de Derecho, Volumen 44, Número 1, Santiago de Chile, abril, 2017. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011

14 CENTRO INTERNACIONAL PARA LA PREVENCIÓN DE LA CRIMINALIDAD, Informe Internacional, Prevención de la criminalidad y seguridad cotidiana: Prevenir la ciberdelincuencia, 2018, p.126. Disponible en: https://cipc-icpc.org/es/informe/informes-internacionales/6o-informe-internacional-sobre-la-prevencion-de-la-criminalidad-y-la-seguridad-cotidiana-prevenir-la-ciberdelincuencia/

15 MIRÓ LLINARES, Fernando. "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", op.cit; p.76

Para que pueda cometerse un ciberdelito debe existir un ciberdelincuente potencialmente motivado para cometer un delito, éste debe ser técnicamente capaz de intentar un ciberataque de algún tipo, su ataque debe alcanzar con éxito su objetivo sin ser bloqueado por tecnologías defensivas, y hay un elemento humano que requiere que un receptor humano final caiga presa del ciberataque que les llega[16].

Sin dudas la ciberdelincuencia es una modalidad de delincuencia especialmente vinculada a las oportunidades. Su comisión puede ser explicado cuando tres elementos o circunstancias coexisten: un agresor motivado, un objetivo adecuado y ausencia de guardianes adecuados. La coincidencia de circunstancias trae consigo la comisión de los ciberdelitos.

a. Agresor motivado: Para que tenga lugar el fenómeno de la ciberdelincuencia solo es necesaria la interacción entre la víctima y el agresor. Una interacción que, a diferencia del mundo físico, no requiere un contacto físico ni espacial. Al no existir distancias que actúen como barreras y dificulten el contacto entre las personas y sus bienes, entre los agentes motivados y los objetivos adecuados, el potencial número de los que pueden acabar siendo ciberdelincuentes y cibervíctimas aumentan.
b. Objetivos adecuados: En el espacio virtual o ciberespacio, el contacto entre personas es distinto. En este caso no es la persona física la que se comunica directamente, en un contexto espacio temporal determinado, con otra persona, sino una representación de la misma por ella definida en base al contenido e información que proyecte o coloque. Existen muchos casos en los que la persona que resulta atacada con el ciberdelito no es la que coloca la información o los bienes en el ciberespacio, pero en otros casos es la víctima la que decide, al incluir información personal en el ciberespacio o compartirla con otros, realizar actividades y situar tales bienes en ese ámbito de riesgo nuevo.

   Con ello se desea transmitir que está en las manos de los usuarios del ciberespacio eliminar del ámbito de ataque aquellos bienes que no incorporen al ciberespacio, de forma tal que, si una víctima no introduce un bien en el ciberespacio, el mismo no estará disponible y no podrá ser objeto del ataque. El crimen, por tanto, en cuanto al objetivo concreto sobre el que se dirige, puede ser evitado por la propia víctima en el ciberespacio desde el momento que no es situado el mismo en el espacio virtual.

   Es necesario recalcar que la introducción de un objetivo en el ciberespacio no en todos los casos se produce de forma voluntaria. En ocasiones se trata de un proceso

[16] Kigerl, Alex, "Interrumpir el proceso de aparición de la ciberdelincuencia: de los delincuentes motivados a los ciberataques", 6to Informe Internacional Prevención de la criminalidad y seguridad cotidiana: Prevenir la ciberdelincuencia, Montreal, 2018. Disponible en: https://cipc-icpc.org/es/informe/informes-internacionales/6o-informe-internacional-sobre-la-prevencion-de-la-criminalidad-y-la-seguridad-cotidiana-prevenir-la-ciberdelincuencia/

casi fortuito, el mero hecho de disponer de un sistema informático y de utilizarlo conlleva la introducción de elementos relacionados con la privacidad que, sin quererlo, pueden conllevar afectaciones a la intimidad o al propio patrimonio. Pero lo cierto es que, en todo caso, el primer condicionante para que un objetivo sea adecuado a los efectos de la fórmula del cibercrimen, es su introducción en el ciberespacio, pues a partir de que un objetivo se introduce en el ciberespacio, voluntaria o involuntariamente, el mismo puede convertirse en adecuado dependiendo de su valoración por parte del agresor motivado.

c. Ausencia de Guardianes capaces del ciberespacio: Navegar por el ciberespacio es una actividad en la que la intervención de los medios de control formal está mucho más diluida. En el ámbito de la cibercriminalidad, guardianes seguros pueden serlo, los sistemas personales, ajenos a la propia víctima o impuestos por ella misma que sirvan como forma de protección, dígase antivirus, cortafuegos, programas anti-spyware o cualesquiera otros sistemas de seguridad. Son los similares en el espacio físico a las alarmas, cerrojos especiales, entre otros. En la prevención de estas conductas la víctima juega un papel preponderante. De ella depende en parte, no sólo su adecuación como objetivo, dada la introducción e interacción de esta en el ciberespacio, sino también su propia autoprotección, pues será ella la que defina los guardianes capaces que la protegerán al tener sistemas antivirus, al actualizarlos, al incorporar otros sistemas de detección de software de riesgo, al actualizar el sistema siempre que se pueda, y mantener una alta percepción el riesgo.

La ciberdelincuencia patrimonial. Nociones para su definición conceptual

No existe un concepto dogmático de ciberdelincuencia patrimonial, no obstante, el término empleado en la investigación para identificar, dentro de la ciberdelincuencia como fenómeno social a aquella que afecta como bien jurídico los derechos patrimoniales, es la de ciberdelincuencia patrimonial. Este término ha sido el asumido en esta investigación, pues en la doctrina no existe un término uniforme, algunos autores emplean el término ciberdelincuencia económica[17], otros el de delitos informáticos de carácter patrimonial[18], por lo que en aras de ser consecuentes con la terminología empleada por

[17] Esta terminología es empleada por autores como Miró Llinares. Vid, Miró Llinares, Fernando, El Cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Madrid, Ediciones Jurídicas y Sociales. S.A, Marcial Pons, 2012.

[18] Esta terminología es empleada por el autor, estudioso de la materia, Romeo Casabona, Carlos María. Muestra de ello lo es su investigación denominada "Delitos Informáticos de carácter patrimonial" publicado en la Revista Informática y Derecho de la Universidad de La Laguna en el año 1996, Vid, Romeo Casabona, Carlos María. "Delitos Informáticos de carácter patrimonial", Revista Informática y Derecho, Universidad de La Laguna, 1996, pp.413-440. Disponible en: https://dialnet.unirioja.es/descarga/articulo/248763.pdf.

la Ley sustantiva, Ley 151/2022 "Código Penal", vigente en Cuba[19], se escogió el término ciberdelincuencia patrimonial.

Una de las expresiones más visibles de la ciberdelincuencia es la que se manifiesta para perjudicar la esfera patrimonial de terceros que pueden ser personas naturales, personas jurídicas o el propio Estado. La ciberdelincuencia patrimonial es la utilización de la informática para la comisión de delitos patrimoniales, son todos aquellos delitos en los que la conducta típica de apropiación, defraudación o daño se lleva a efecto a través de la manipulación fraudulenta de documentos informatizados. Se trata de aquella actuación fraudulenta e ilícita, sobre medios informáticos, para obtener un beneficio provocando el perjuicio de un tercero[20].

Como señala Miró Llinares el cibercriminal económico utiliza la red, los sistemas conectados a ella, la información en ellos contenida, los servicios y cualquier otro elemento de las TIC como medio u objeto para el lucro económico[21].

La ciberdelincuencia patrimonial es, por tanto, un primer gran ámbito de delincuencia en Internet que si bien abarca múltiples tipologías de conducta diferentes entre sí, todas ellas son parte del puzle requerido para lograr el fraude económico final[22]. La peculiaridad del medio empleado en las manipulaciones de datos informatizados y el hecho de que en realidad la acción recae sobre elementos incorporales e intangibles, como pueden ser transferencias, fondos en tarjetas magnéticas, saldo, le otorgan a esta manifestación delictiva características propias.

Análisis de la ciberdelincuencia patrimonial en Cuba desde su configuración jurídico penal

No existe un concepto dogmático de ciberdelincuencia patrimonial, no obstante, el término que se ha empleado en la investigación para identificar, el tipo de ciberdelincuencia que afecta como bien jurídico los derechos patrimoniales, es el de ciberdelincuencia

19 NA: El título de los delitos que protegen los derechos patrimoniales en la Ley 151/2022 "Código Penal" es el Título XVII, el cual se denomina delitos contra los derechos patrimoniales. Bajo este título están recogidos los delitos de Hurto, Sustracción de electricidad, gas, agua o fuerza, Sustracción de vehículos de motor para usarlos, Robo con violencia o intimidación en las personas, Robo con fuerza en las cosas, Tenencia, fabricación y venta de instrumentos idóneos para ejecutar el delito de robo, Extorsión, Chantaje, Usurpación, Ocupación o disposición ilícita de locales o viviendas, Estafa, Apropiación Indebida, Receptación, Daños. Vid, Asamblea Nacional del Poder Popular, Ley 151/2022 "Código Penal". Gaceta Oficial No. 93 Ordinaria de 1ro. de septiembre de 2022, República de Cuba, Ministerio de Justicia.

20 Corcoy Bidasolo, Mirentxu, "Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", Cuaderno del Instituto Vasco de Criminología, Número 21, 2007, p.16.

21 Miró Llinares, Fernando, El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Madrid, Ediciones Jurídicas y Sociales. S.A, Marcial Pons, 2012, p.119.

22 Ídem, p.122

patrimonial. Ello obedece a un criterio de uniformidad y correspondencia con la terminología empleada por la Ley 151/2022, "Código Penal", vigente en Cuba.

El Título de la referida ley penal que tiene por base la protección del patrimonio como bien jurídico específico se distingue o clasifica en: a) Delitos contra los derechos patrimoniales por sustracción, entre los que se incluyen: Hurto; Sustracción de Electricidad, gas, agua o fuerza; Sustracción de vehículos de motor para usarlos; Robo con Violencia o intimidación en las personas; Robo con Fuerza en las cosas; Tenencia, fabricación y venta de instrumentos idóneos para ejecutar el delito de robo; Extorsión y Chantaje; Usurpación; Ocupación o disposición ilícita de locales o viviendas, b) Delitos contra los derechos patrimoniales por defraudación, comprendiendo: Estafa; Apropiación Indebida; Receptación y c) Delitos contra los derechos patrimoniales por daños[23].

Haciendo un análisis dogmático de los tipos penales patrimoniales que recoge la Ley penal cubana debe decirse que no todas las conductas en el título dedicado a proteger los derechos patrimoniales pueden ser cometidas a través de las TIC. Por lo que no todos los tipos penales encontrarán en la ciberdelincuencia patrimonial cabida, pues, por su propia naturaleza, no pueden ser llevados a cabo mediante el empleo de TIC.

En este sentido advierte el autor González Rus que en el delito de Hurto no es posible su comisión mediante TIC pues el Hurto implica apropiarse de una cosa mueble, entendiéndose esta como cosa corporal en las que sea posible su aprehensión o apoderamiento material, quedando excluidas las incorporales o inmateriales[24].

Una conducta delictiva semejante a la antes planteada es la utilización de tarjetas magnéticas de terceros usadas sin consentimiento del titular o robadas, pero en este caso estaríamos ante el delito de Robo con fuerza en las cosas, específicamente previsto en el artículo 416.1 inciso b) del Código Penal[25]. Este delito considera "llaves" a las tarjetas magnéticas o perforadas, los mandos o instrumentos de apertura a distancia, a las contraseñas, accesos u otras aplicaciones informáticas similares. Con solo leer el articulado se vislumbra que la ciberdelincuencia patrimonial tiene total cabida aquí.

---

23 Esta clasificación se advierte en Goite Pierre, Mayda, "Delitos contra los derechos patrimoniales" en Colectivo de Autores, Derecho Penal Especial, Tomo II, Editorial Félix Varela, La Habana, 2005, pp. 198 y 199.

24 Vid, González Rus, Juan José, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", Revista de la Facultad de Derecho de la Universidad Complutense, ISSN 0210-1076, Número Extra 12, 1986, pp. 107-164

25 Artículo 416.1. Se sanciona con privación de libertad de tres a ocho años a quien sustraiga una cosa mueble de ajena pertenencia, con ánimo de lucro, concurriendo en el hecho cualquiera de las circunstancias siguientes: b) uso de llave falsa, o de la verdadera que hubiese sido sustraída o hallada, o de ganzúa u otro instrumento análogo; a tales efectos, se consideran como llaves, las tarjetas magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y las contraseñas, accesos u otras aplicaciones informáticas similares. Vid, Asamblea Nacional del Poder Popular, Ley 151/2022 "Código Penal", op. cit.

Por otro lado, el delito de Estafa protege como bien jurídico al patrimonio, pues se refiere al término general de "bienes"[26] considerado en su totalidad, por lo que se encuentran con protección no solo las cosas muebles sino las inmuebles, como pueden ser valores intangibles, derechos, crédito. Este tipo delictivo se caracteriza por el engaño y el error al que es inducido un individuo por el autor, por lo que siempre que estemos ante manipulaciones informáticas, particularmente cuando se realizan en la fase de la programación o procesamiento de los datos, sin la intervención de persona alguna a la que realmente se engañe y se induzca a error estaremos ante un Robo con Fuerza en las Cosas, y no una Estafa.

La Estafa por medios informáticos es una de las tipologías de la ciberdelincuencia en el que existe una defraudación empleando medios informáticos, es decir, la utilización del sistema informático es el medio para transferir los activos patrimoniales a favor del autor, y este desplazamiento es siempre virtual[27]. Sus elementos clásicos son[28]:

- El ánimo de lucro concebido como la pretensión del autor del hecho.
- Empleo de ardid o engaño
- El error o situación de error de quien sufre el engaño, es decir, consecuencia a la que conduce el previo comportamiento engañoso o fraudulento
- La producción de un acto de disposición patrimonial consecuencia de la situación de error al que le induce el sujeto activo.
- El perjuicio patrimonial constituye el auténtico resultado del delito.

El delito de Apropiación Indebida, por su parte, establece que será responsable del mismo quien, con el propósito de obtener una ventaja o un beneficio patrimonial ilegítimo, para sí o para otra persona, se apropie o consienta que otro se apropie de bienes que le hayan sido confiados por cualquier título que conlleve obligación de entrega o devolución. Cabría analizar si serán responsables los funcionarios del banco que con razón de su cargo y función tienen la disponibilidad de los fondos, claves y contraseñas de las cuentas bancarias

[26] Artículo 423.1. Quien, con el propósito de obtener para sí o para otra persona, una ventaja o un beneficio patrimonial ilegítimo, y empleando cualquier ardid o engaño bastante o suficiente que induzca a error a la víctima, determine a esta a realizar o abstenerse de realizar un acto en detrimento de sus bienes o los de un tercero, incurre en sanción de privación de libertad de seis meses a un año o multa de cien a trescientas cuotas, o ambas. Vid, Asamblea Nacional del Poder Popular, Ley 151/2022 "Código Penal", op. cit.

[27] Vid, García García-Cervigón, Josefina, "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, Número 74, mayo-agosto 2008, p.292. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=289096

[28] Mata y Martín, Ricardo, Delincuencia informática y Derecho Penal, Editorial Hispamer, Nicaragua, 2003, p.50 - 52.

de los usuarios. Sin embargo, coincido con Romeo Casabona[29]en que esto no ocurriría respecto a estas, pues estos no ejercen la custodia o administración del dinero u otros bienes, ni toman decisiones sobre los mismos, pero es cierto que tienen de una u otra forma acceso a los datos informatizados como consecuencia de su actividad profesional.

Tendencias del fenómeno de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba

De las modalidades de ciberdelincuencia patrimonial en Cuba destaca, por ser la más usual, la Estafa Informática, ya sea mediante la suplantación de la identidad del usuario a partir de datos que proporciona el mismo, o que se obtiene mediante el engaño para que comparta datos como el pin, número de las tarjetas magnéticas, contraseña, nombres y apellidos del dueño de la cuenta, carnet de identidad, fotos, capturas de pantalla de las últimas operaciones registradas en Transfermóvil, o mediante el hackeo de las cuentas de los usuarios, utilizando la técnica del phishing.

El fenómeno delictivo en cuestión tuvo su alza en el 2021 como reflejo del cambio de la moneda y la informatización de la sociedad. En una nota compartida por el Banco Central de Cuba (BCC) se explica que los fraudes se han concretado al realizar transferencias de efectivo a personas desconocidas y que, además, poseen perfiles falsos en redes sociales, sobre todo en Facebook.

Los principales modos de operar para llevar a cabo las Estafas Informáticas en Cuba son la Ingeniería Social y, dentro de esta, la más común es la técnica del Phishing. En ambos casos el ciberdelincuente busca obtener información personal y confidencial de su víctima o lograr que esta realice disposiciones patrimoniales, manipulándola o engañándola mediante la suplantación o utilización de falsa de identidad, a través del empleo de datos, que previamente conoce y que puede usar para ganarse la confianza de estas, o utilizando atractivas ofertas laborales, promociones, inversiones, venta de artículos, enlaces electrónicos, entre otros ardides, para lo cual presentan formularios que deben llenar los usuarios con contenido y datos confidenciales.

Pero lo cierto es que, además, de estas técnicas el ciberdelincuente obtiene esa información en bases de datos en internet que no están protegidas con medidas de seguridad y que las personas, por desconocimiento o falta de precaución, piensan que nunca serán utilizados por terceros sin su consentimiento.

Actualmente en Cuba los métodos más comunes empleados por los ciberdelincuentes para llevar a cabo conductas que afectan al patrimonio de personas naturales son:

[29] Romeo Casabona, Carlos María, "Delitos Informáticos de carácter patrimonial. Revista Informática y Derecho". Universidad de La Laguna, 1996. Disponible en: https://dialnet.unirioja.es/descarga/articulo/248763.pdf

1. El SMS de confirmación de pago: Transfermóvil es la aplicación de pago más utilizada en Cuba para el comercio digital, y esta plataforma usa el envío de mensajes de texto (SMS) y códigos USSD para su funcionamiento, características de las cuales se aprovechan los ciberdelincuentes para engañar a sus víctimas. Una forma de estafa recurrente es el recibo de un SMS de confirmación de pago. Normalmente, cuando una persona realiza una transferencia puede agregar un número de teléfono al cual llega un SMS confirmando la transferencia. Esta forma de estafa está siendo muy utilizada, sobre todo, utilizando como cebo el intercambio de divisas. Todo comienza con el anuncio tentador de compra o venta de divisas por las redes sociales Facebook, Telegram, WhatsApp, Revolico, un anuncio casi siempre desde un perfil falso. Cuando el usuario contacta el ciberdelincuente envía a este un SMS idéntico al que envía Transfermóvil como si hubiese realizado el pagado, y la víctima realiza la transferencia del efectivo para cerrar el negocio.
2. El Amigo falso de Facebook: Otro engaño digital para estafar saldo móvil aprovecha las redes sociales para buscar posibles víctimas. El hacker se crea un perfil falso haciéndose pasar por un amigo de la persona objetivo y lo convence de que se le presentó un problema grande y necesita saldo móvil con urgencia, o alguna transferencia de efectivo.
3. SMS equivocado: Es otro tipo de estafa para robar saldo móvil se apoya en los mensajes de texto. El atacante envía un SMS haciéndose pasar por ETECSA. El mensaje recrea el texto que envía la empresa cubana cuando se realiza una transferencia de saldo. Acto seguido, el estafador envía otro SMS o la llamada en el que asegura que realizó una transferencia por una equivocación en el número de teléfono y pide de favor que le devuelvan su saldo.
4. Enlace engañoso: El ciberdelincuente envía un enlace al usuario con contenido tentador y cuando este abre el enlace para tener acceso al contenido, le piden ingresar nuevamente los datos de nombre de usuario y contraseña. En el momento en el que estos datos son ingresados nuevamente, los hackers guardan esta información para entrar a las cuentas de los usuarios y buscar información útil además de embaucar a sus contactos con el mismo mensaje, con el objetivo de obtener un beneficio económico, empleando la técnica del phishing pues buscan ganarse la confianza del usuario mediante el envío de un mensaje que enviaría alguien conocido. Ejemplo de esta forma de operar fue el famoso enlace denominado "¿Eres tú quien aparece en el video?"[30].
5. Los "cambietazos" de divisas, empleando como cebo a mujeres jóvenes sin antecedentes penales, de buena conducta, son contratadas por vía digital por el autor de las defraudaciones, quien es desconocido para ellas, para que, en representación suya,

[30] Vid, Cubadebate, "¿Eres tú en el video? No abras el link de Messenger", 5 de abril del 2022. Disponible en: http://www.cubadebate.cu/noticias/2022/04/05/eres-tu-en-el-video-no-abras-el-link-de-messenger/

participe en compra venta de divisas con la persona que resulta ser afectada. En el contrato inicial que conciertan, vía digital, con el defraudador, estas jóvenes llenan una especie de formulario, donde facilitan sus datos de identidad, datos bancarios y contraseñas a solicitud del presunto empleador, quien les hace creer que se desempeñarán como gestoras de cobro en las operaciones de compra y venta de moneda dura. Al momento de la transacción, el tercero con el que acuerda el defraudador, previamente y vía on line la operación de cambio, transfiere el dinero en presencia de estas jóvenes, y una vez las jóvenes informan del éxito de la transferencia al defraudador, estas resultan bloqueadas de acceder a su cuenta, y el defraudador se apropia del dinero que estas poseían y del dinero transferido por las víctimas.

6. Utilización de herramientas digitales que burlan barreras de seguridad, las cuales adquieren de grupos clandestinos especializados en temas de hackeo, que existen en las redes sociales Telegram y WhatsAp, dirigidos fundamentalmente a la creación de programas informáticos capaces de sustraer informaciones bancarias, tanto en sitios de comercio electrónico como en pasarelas de pago y al escaneo y explotación de vulnerabilidades en plataformas web. Siendo así, con el fin de descubrir fisuras de la seguridad en las plataformas de instituciones estatales, económicas y militares cubanas y obtener información sobre su funcionamiento y los usuarios que la emplean, los ciberdelincuentes utilizan esas aplicaciones digitales, obteniendo los datos sin autorización de los usuarios legítimos, luego acceden a las cuentas con dicha información, cambian los accesos y contraseñas y transfieren, escalonadamente, la cuantía deseada a cuentas bancarias que utilizan como puentes.

Análisis criminológico de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba

Para llevar a cabo el análisis criminológico de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba se tomaron como referencia los casos de ciberdelincuencia patrimonial aportados por la Fiscalía General de la República, el Departamento de Control al Órgano Especializado de Investigación Criminal de los Delitos Comunes de la Fiscalía Provincial de la Habana y las Unidades Territoriales de Investigación Criminal No. I y No. III, además, se tomaron en cuenta las respuestas de las encuestas aplicadas a usuarios de las redes y los resultados de las entrevistas realizadas a especialistas en la materia. Para exponer el resultado obtenido se tuvieron como parámetros los siguientes elementos: características del imputado, características de las víctimas, las oportunidades delictivas que propiciaron el hecho y los obstáculos enfrentados durante la fase investigativa del delito.

a. En cuanto a las características de los ciberdelincuentes: En los procesos donde la investigación permitió llegar al ciberdelincuente se evidenció que en el actuar de estos expusieron motivaciones económicas, sociales o personales. En los casos estudiados los comisores de los hechos actuaban con evidente ánimo de lucro,

pero también asumía sus hechos como un evidente reto personal de superación. En la mayoría de los casos los ciberdelincuentes eran hombres jóvenes, con edades de entre 18 y 35 años de edad, con una formación empírica, en la informática, pero muy hábiles, con interés y curiosidad en la informática, las redes y el mundo virtual. La casi totalidad de ellos carente de antecedentes penales, y se trataba de individuos desocupados laboralmente. Se trata de personas que aprenden a navegar por la red y a delinquir a través de páginas webs, blogs o foros, por lo que, aunque en la mayoría de los casos son personas con conocimientos no suelen haber recibido formación profesional. Tampoco existe una relación entre el nivel educacional o cultural y el perfil de los ciberdelincuentes. Se trata de personas dispuestas a aprender, con elevada autoestima y seguras de sí misma.

Durante el estudio de los casos se advirtió que estos muchachos comenzaron su actividad motivados por la curiosidad, por lo que tanteaban por los sistemas informáticos, luego de detectar las vulnerabilidades de los mismos, o llevando al error a los usuarios de las redes, lo cual refuerza la idea de que el ciberdelincuente se aprovecha de las brechas de seguridad en los sistemas informáticos y de la colaboración involuntaria de sus víctimas.

b. Características de las víctimas: Para hacer referencia a este punto del estudio, es necesario aclarar que la mayoría de las personas que han resultados víctimas específicamente de las estafas informáticas son personas no nativas digitales, con acceso a internet, cuentas bancarias activas, que usualmente operan con las plataformas de pago, y que realizan un uso inadecuado de los sistemas informáticos, actúan con ingenuidad y desconocimiento de los riesgos, ejemplo de ello es la poca protección de sus activos, por ejemplo contraseñas muy fáciles de memorizar. Por otro lado, cuando se trata de los robos con fuerza en las cosas cometidos luego de forzar sistemas informáticos, se aprecia que la víctima puede ser cualquier usuario de la red, de cualquier edad. Aquí las víctimas no participan en la cadena causal que da al traste con la sustracción del patrimonio, ellas no contribuyen con su actuar al resultado delictivo.
c. Oportunidades delictivas: Las características del ciberespacio constituyen una de las oportunidades delictivas que propician los hechos de ciberdelincuencia, entre ellas, el alcance del ciberespacio, debido a la ausencia de fronteras posibilita que una acción iniciada en un punto termine afectando de forma casi instantánea a elementos situados en cualquier parte del mundo; la asimetría de este espacio, dado a que el acceso al ciberespacio es global, sencillo y económico, tal es así que un individuo o pequeña organización pueden, con un mínimo de capacidad técnica y recursos, producir efectos en un oponente con el que se guarda total desproporción; y el anonimato pues la utilización de identidades virtuales facilita la ocultación de la verdadera personalidad e intenciones de individuos o grupos. Son fenómenos frecuentes usurpar la identidad de terceros para ocultar las actividades

propias, lo cual tributa a que la atribución de estas actividades se convierte en un problema fundamental, siendo necesario combinar múltiples disciplinas del área de la Inteligencia y del análisis forense para lograr resultados.

El grado de sofisticación del ejecutante incrementa la dificultad de la atribución de responsabilidad e incluso puede hacerla imposible. Esto a su vez constituye una de las oportunidades delictivas, pues dificulta el control social formal de este tipo de delitos y con ello se favorece la impunidad de estas conductas, lo cual es una circunstancia que motiva al ciberdelincuente a operar sin el riesgo de ser capturado.

Cabe destacarse también la ingenuidad, el exceso de confianza y el desconocimiento que demuestran la baja percepción del peligro en los usuarios de las redes y víctima de estos delitos, constituyendo esta una oportunidad delictiva que favorece las manifestaciones de ciberdelincuencia patrimonial en Cuba. Por otro lado, las brechas de seguridad en los sistemas bancarios nacionales y en los sistemas de ciberseguridad de instituciones, organizaciones y entidades estatales y no estatales constituyen una vulnerabilidad peligrosa que deviene en oportunidad delictiva.

d. Obstáculos investigativos enfrentados: Resulta muy difícil la investigación de sus actos y su demostración, dado el carácter técnico y sofisticado de este tipo de delitos. Para el esclarecimiento del hecho es de vital relevancia la información aportada por los propios imputados, quienes dan información respecto a la dinámica del hecho. Elementos sin los cuales resultaría muy difícil reconstruir el hecho para describir la conducta por él realizada para producir el resultado delictivo.

Como vulnerabilidades en las investigaciones se aprecia que existe falta de conocimientos informáticos, falta de preparación en la investigación de estos delitos, falta de herramientas investigativas específicas para esta tipología delictiva, así como se carece de una metodología que indique como ordenar lógica y metodológicamente la investigación en aras de optimizar los recursos y no perder tiempo. Ello indica fallas en el control social formal, que vienen dadas especialmente por la falta de un sistema de enfrenamiento adecuado y preparado para enfrentar estas conductas delictivas.

Propuestas para disminuir los riesgos de ocurrencia de la ciberdelincuencia patrimonial a partir del análisis de sus oportunidades delictivas

Además de los costos económicos de la ciberdelincuencia patrimonial, existen impactos menos tangibles, incluyendo la pérdida de confianza en el comercio electrónico, la erosión de la privacidad individual y la disminución de la confianza en los servicios en línea. Ello unido a la gravedad de no accionar frente a un fenómeno en auge, que muestra señales de su significación social, incluso al nivel de constituir un problema de seguridad nacional, hace que sea imprescindible diseñar estrategias de prevención de este fenómeno.

Es reconocido que las personas son el eslabón más débil de la cadena de la seguridad. Ello implica que, aunque tradicionalmente el abordaje analítico de la problemática ha

estado dirigido al diseño de soluciones orientadas fundamentalmente hacia las infraestructuras de comunicación, los dispositivos y las aplicaciones, se ha olvidado que el factor humano es un elemento activo para garantizar la seguridad[31]. Es por ello que debe trabajarse en función de que las personas usuarias de las redes dejen de ser sujetos pasivos que necesitan ser protegidas para convertirse en agentes activos, en guardianes de su seguridad, y la seguridad de su información, datos y sistemas informáticos.

Es necesario trabajar en la prevención general y en la educación ciudadana frente al fenómeno. Ello deberá partir de la exposición del alcance e incidencia de dicha tipología delictiva en Cuba, debe crearse una cultura de cómo evitar ser víctima de estos delitos, cómo proteger los datos personales y qué hacer en caso de ser víctima de estos. El punto de partida debe ser el entendido de que la baja percepción del riesgo en la población usuaria de las redes, la ingenuidad y el desconocimiento constituyen una de las principales oportunidades delictivas que propician este tipo de manifestaciones, lo que demuestra que es necesario elevar la percepción de riesgo respecto a estos ilícitos en la población, mediante estrategias de comunicación y educación.

En este sentido es recomendable instruir a los usuarios de las redes en que deben abstenerse de aportar datos personales a desconocidos o colocarlos en plataformas de redes sociales, pues estas luego son utilizadas por los ciberdelincuentes como fuente de información y selección de las víctimas; deben chequear sistemáticamente las cuentas personales; deben utilizar el doble factor de autenticación[32], que es una medida de seguridad que sirve para verificar la identidad de la persona que quiere ingresar a una cuenta, que requiere además de la contraseña habitual un código de seguridad adicional; deben emplear contraseñas fuertes, que son aquellas contraseñas seguras en las que combinan números, letras y símbolos, incluyen de 16 a 20 caracteres y no se comparten con nadie; deben atender las alertas, vía correo electrónico, sobre intentos de acceder a sus cuentas por dispositivos distintos a los usualmente utilizados, elementos que deben tenerse en cuenta, porque constituyen mecanismos de seguridad que blindan las cuentas e impiden el acceso de terceras personas; no deben hacer clic en enlaces sospechosos y deben ser cautelosos con los correos electrónicos y mensajes inesperados; no deben guardarse las claves o contraseñas junto con sus tarjetas; no deben hacer pública información impresa en las tarjetas; no deben informar a desconocidos datos del carné de identidad, número, tomo o folio.

---

31 Sánchez Vera, Fulgencio; Javier Eloy, Martínez Guirao; y Anastasia, Téllez Infantes, "La seguridad en el ciberespacio desde una perspectiva sociocultural", Methaodos, Revista de Ciencias Sociales, 2022, Volumen 10, Número 2, p.244. Disponible en: https://doi.org/10.17502/mrcs.v10i2.577

32 Existen distintas formas para generar los códigos de autenticación: por mensaje de texto en un teléfono móvil enviado por el servicio al que se desea conectar, aplicaciones de doble autenticación para que sea más inmediato, también hay otras formas de hacerlo, como a través de preguntas de seguridad, número de teléfono, factor biométrico como una huella dactilar, rostro, voz o retina, entre otros sistemas que se pueden usar. Blog de Actualidad de la transformación digital. Disponible en: https://ginzo.tech/doble-factor-autenticacion/

En otro sentido es necesario recalcar que la rápida evolución de las TIC ha propiciado que la ciberseguridad resulte una condición fundamental para garantizar el desarrollo seguro de actividades básicas en la sociedad moderna. Es por ello que es necesario trabajar y reforzar ciberseguridad de las plataformas y sistemas digitales, en Cuba pues constituyen las brechas de seguridad uno de las oportunidades delictivas que, actualmente, propician las manifestaciones ciberdelictivas. Debe diseñarse un correcto sistema de ciberseguridad en las entidades estatales y no estatales, y reforzar aquellas que aún presentan vulnerabilidades. Ello debe partir de reconocer que proteger la información y los sistemas informáticos ante las amenazas de las que son vulnerables, es una tarea de suma importancia, que se vincula con la seguridad de la información que se maneje y circule por las redes de entidades, las cuales pueden alcanzar a los usuarios, clientes y la nación.

La ciberseguridad constituye la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las instituciones tienen la responsabilidad de proteger los datos, dispositivos, servidores y las redes frente a posibles amenazas. Para ello deben utilizar medidas y herramientas de ciberseguridad que garanticen la protección de los datos confidenciales del acceso no autorizado e interrupciones en las operaciones debido a una actividad de red no deseada. El éxito de un ciberataque produce la exposición, sustracción, eliminación o alteración de datos confidenciales. Para la implementación de estrategias de ciberseguridad debe contarse con especialistas de ciberseguridad, que evalúen los riesgos de seguridad de los sistemas informáticos existentes, redes, almacenamiento de datos, aplicaciones y otros dispositivos conectados, y que, a partir de los análisis, creen un marco de ciberseguridad integral e implementan medidas protectoras en la entidad.

Es por ello que se requiere de un equipo de especialistas, capacitados, que cuenten con las herramientas técnicas, tecnológicas para desarrollar un adecuado sistema de ciberseguridad, en el que se empleen tecnologías de defensa cibernética constituido por varias capas de protección contra posibles amenazas en todos los puntos de acceso a datos, capaces de identificar el riesgo, proteger identidades, infraestructura y los datos, detectar anomalías, responder y analizar la causa raíz y realizar la recuperación después de un evento de ciberataque. Por otro lado, la formación y educación de los empleados con respecto a los principios de ciberseguridad reduce los riesgos de descuidos que pueden dar lugar a incidencias no deseadas.

Una cuestión a tener en cuenta lo constituyen los aspectos relacionados con el control social formal e informal. En este sentido, publicitar el trabajo que realiza el país en aras de desarrollar estrategias de ciberseguridad, exponer los casos de ciberdelincuencia que se susciten en el país, cómo se investigan y esclarecen estos hechos, así como mostrar las consecuencias jurídico penales de los responsables puede servir de freno inhibitorio a los ciberdelincuentes, máxime cuando se ha advertido que una de las oportunidades delictivas en este tipo de conductas es la confianza en la impunidad de sus conductas.

En este orden de ideas, implementar una correcta estrategia comunicativa en la que se instruya a la población en la ciberseguridad, en cómo protegerse de ciberataques y en cómo reaccionar ante estas conductas, sobe la base de lo perjudicial que pueden llegar a ser contribuirá a fomentar en estas personas una cultura de repudio a estas conductas lesivas, lo cual influirá en la labor de rechazo y enfrentamiento a estas conductas.

Conclusiones

En el marco del proceso de informatización de la sociedad Cuba disfruta los beneficios que la apertura al mundo digital trae consigo, sin embargo, también enfrenta los impactos negativos del uso de estas tecnologías. Es precisamente por lo novedoso y complejo de este proceso de digitalización de la sociedad que la ciudadanía no ha podido adquirir las habilidades de ciberseguridad y protección de sus datos personales, haciéndose imperiosa la necesidad de educar y proteger a la misma, mediante el desarrollo de estrategias preventivas eficaces que combinen el trabajo educativo de la población con el fortalecimiento de los mecanismos de ciberseguridad y del sistema de enfrentamiento.

Tener en cuenta los presupuestos criminológicos que permiten el abordaje de la ciberdelincuencia patrimonial que afecta a personas naturales en Cuba significa entender el fenómeno, sus causas, sus consecuencias y son el cimiento necesario para el diseño e implementación de estrategias preventivas eficaces. Es en vista a este fin que el estudio ha pretendido ser un acercamiento criminológico al fenómeno en Cuba, toda vez que se trata de un asunto que va adquiriendo interés por el incremento que ha experimentado y sus consecuencias, en una nación que se abre digitalmente. Todo ello siendo conscientes de que la solución no será jamás frenar el desarrollo tecnológico sino direccionarlo de una forma segura, previniendo y enfrentando todo ataque o riesgo en este empeño. Algo que, necesariamente, deberá partir del diseño de un sistema de ciberseguridad robustecido y el desarrollo de una cultura, educación y concientización digital de la población.

Bibliografía

Fuentes doctrinales

Acosta, María Gabriela; Merck, Milko Benavides, y Nelson, Patricio García, "Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios", Revista Venezolana de Gerencia, Volumen 25, Número 89, 2020.

Aguilar Cárceles, Marta María, "Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido", Revista Criminalidad, Volumen 57, Número 15, 2015. Disponible en: https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/view/165

Agustina Sanllehí, José, "La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual", Revista International e-Journal of Criminal Sciences, Artículo 4, Número 3, 2009.

Anguita Osuna, José Enrique, "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea", Revista de Estudios en Seguridad Internacional, Volumen 4, Número 1, 2018, pp. 107-126. Disponible en: http://dx.doi.org/10.18847/1.7.7

Atiénzar Rivero, Enrique, Estafas entre redes, Cubadebate, 16 de abril del 2023. Disponible en: http://www.cubadebate.cu/especiales/2023/04/16/estafas-entre-redes/

Benito, María, "Ciberdelincuencia: ¿qué es y cómo combatirla?", Blog de los Estudios de Derecho y Ciencia Política, IurisCrimPol, 15 de junio del 2023. Disponible en: https://blogs.uoc.edu/edcp/es/ciberdelincuencia-que-es-y-como-combatirla/

Blog de Actualidad de la transformación digital. Disponible en: https://ginzo.tech/doble-factor-autenticacion/

Borrego, Mary Luz, "Estafas virtuales: en la confianza está el peligro", Periódico Escambray, 10 de marzo del 2022. Disponible en: https://www.escambray.cu/2022/estafas-virtuales-en-la-confianza-esta-el-peligro/

Bueno De Mata, Federico, Prueba electrónica y proceso 2.0, Editorial Tirant lo Blanch, Valencia, 2014.

Cabrera Cabrera, Xiomara, "La prevención victimológica en Cuba. Insuficiente protección del Derecho Penal", Revista Contribuciones a las Ciencias Sociales, marzo 2012. Disponible en: https://ideas.repec.org/a/erv/coccss/y2012i2012-0318.html

Cabrera Quiroz, Marycarmen, "Fundamentos jurídicos considerados por los fiscales penales del cercado de Cajamarca para archivar las investigaciones de delitos informáticos durante el período 2010-2018", Repositorio de la Universidad Privada del Norte. Disponible en: https://hdl.handle.net/11537/24533

Cámara Arroyo, Sergio, "Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente", Revista Derecho y Cambio Social, Número 60, abril-junio 2020.

Campoy Torrente, Pedro y Lucia, Summers, "Los precipitadores situacionales del delito: otra mirada a la interacción persona-ambiente", Revista Criminalidad, Volumen 57, Número 3, 2015.

Castells, Manuel, La era de la información. Fin de milenio, Madrid: Alianza editorial, 1998.

Castro Espina, Sandra Jeannette, Algunos aspectos dogmáticos de la delincuencia informática, 2007. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3313831.pdf

Catá del Palacio, Arturo, Ciberdelincuencia. Desarrollo y persecución tecnológica. Universidad Politécnica de Madrid, 2014. Disponible en: https://oa.upm.es/34795/

Ciberdelincuencia: tipos y medidas de prevención, 17 de enero 2022. Disponible en: https://www.redseguridad.com/actualidad/cibercrimen/que-es-la-ciberdelincuencia-y-como-se-puede-prevenir_20220117.html

Corcoy Bidasolo, Mirentxu, "Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos", Cuaderno del Instituto Vasco de Criminología, Número 21, 2007.

Cordero Ruiz, Nuria Fernanda, La ciberdelincuencia, Máster Universitario en Acceso a la Profesión de Abogado Universidad de Alcalá, 2021. Disponible en: https://ebuah.uah.es/dspace/handle/10017/49563

Cubadebate, "¿Eres tú en el video? No abras el link de Messenger", 5 de abril del 2022. Disponible en: http://www.cubadebate.cu/noticias/2022/04/05/eres-tu-en-el-video-no-abras-el-link-de-messenger/

De Armas Fonticoba, Tania y Ángela, Gómez Pérez, Introducción a la Criminología. Editorial Félix Varela, La Habana, 2015.

De la Cuesta Arzamendi, Jorge Luis y Ana Isabel, Pérez Machío, "Ciberdelincuentes y Cibervíctimas" en Derecho penal informático. Pamplona: Civitas y Thomson Reuters. Disponible en: https://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimas.pdf

De Pedro Baena, Nerea, ¿Cómo es el perfil del ciberdelincuente? Boletín semanal Lisa News, 2022. Disponible en: https://www.lisanews.org/ciberseguridad/como-es-el-perfil-del-ciberdelincuente/

Del Sol González, Yaditza, "Wifi falsa y otros delitos en la red cubana", La Habana, Periódico Granma, 12 de junio del 2024.

Diario de la Juventud cubana. Periódico juventud rebelde, 17 /6/2022. Disponible en: https://www.juventudrebelde.cu/cuba/2022-06-22/mas-de-7-5-millones-de-cubanos-con-internet

Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución. El Convenio de Budapest", Revista Electrónica de Derecho de La Universidad de la Rioja (REDUR), Número 8, 2010, pp. 169-203. Disponible en: https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071

Díaz Hernández, Rosa M. y Zulariam, Pérez Martí, "Estafa en la WiFi: Robo de cuentas y otros ciberdelitos en Cuba", Cubadebate, 17 de diciembre del 2017. Disponible en: http://www.cubadebate.cu/especiales/2017/12/17/estafa-en-la-wifi-robo-de-cuentas-nauta-y-otros-ciberdelitos-en-cuba/

División de Aplicaciones TIC y Ciberseguridad. Departamento de Políticas y Estrategias. Sector de Desarrollo de las Telecomunicaciones de la UIT, "El ciberdelito: Guía para los países en desarrollo", Proyecto de abril de 2009. Disponible en: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

Espinosa Bejerano, Santiago, La ciberseguridad, el ciberespacio, internet y las tecnologías de la información y las comunicaciones. Disponible en: http://www.cubadebate.cu/especiales/2021/09/04/la-ciberseguridad-el-ciberespacio-internet-y-las-tecnologias-de-la-informacion-y-las-comunicaciones/

Evaristo Abril, Domingo; Miguel, López-Coronado; Rafael, Mompó Gómez, "La Necesidad de Indicadores Sociales y Económicos para el Estudio de la Evolución de la Sociedad de la Información", Revista de investigación económica y social de Castilla y León, ISSN 1575-5835, Nº 1, 1999, pp. 73-86.

Fernández Romo, Rodolfo y Waldemar, Paulo Da Silva José, "Aristas criminológicas de la delincuencia informática", Serie Ciencias Penales y Criminológicas Interrogantes, Alternativas y Desafíos en Clave de Derecho Penal y Criminología. Disponible en: https://cuba.vlex.com/vid/aristas-criminologicas-delincuencia-informatica-690582601

García García, Diego Eloy, "El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016)", Revista Boliviana de Derecho,

Número 25, Santa Cruz de la Sierra, 2018. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100025

García García, Gelsy, "Acceso y uso de las Tecnologías de la Información y Comunicación en la Cuba actual" , Revista de Estudios del Desarrollo Social: Cuba y América Latina, Volumen 3, Número 2, mayo-agosto, 2015, pp. 1-53. Disponible en: https://www.redalyc.org/pdf/5523/552357189011.pdf

García García-Cervigón, Josefina, "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, Número 74, mayo-agosto 2008. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=289096

GIL, Leandro (Coord.). Cibercrimen y Delitos Informáticos. Guía de Estudio, año 2021. Disponible en: https://www.mseg.gba.gov.ar/areas/Vucetich/MANUALES%20DE%20MATERIAS%202022/MANUAL%20Cibercrimen%20y%20delitos%20inform%C3%A1ticos.pdf

Goite Pierre, Mayda, "Delitos contra los derechos patrimoniales" en Derecho Penal Especial, Colectivo de Autores, Tomo II. Editorial Félix Varela, La Habana, 2005.

Goite Pierre, Mayda; Rodolfo, Fernández Romo; Francisco Marcelo, Obando Freire; Andrés, Obando Ochoa y Santiago Velásquez Velásquez, "La prevención situacional del delito", Serie Ciencias Penales y Criminológicas El Derecho Penal y la Criminología. Su Práctica en Angola, Cuba y Ecuador en el Siglo XXI, julio 2019. Disponible en: https://cuba.vlex.com/vid/prevencion-situacional-delito-844293915

Gómez Pérez, Ángela, "Aspectos puntuales acerca de la Victimología", Tema VII en Manual de Criminología, Colectivo de Autores, Editorial Félix Varela, La Habana, 2004.

González Fuentes, Yisel, "¿Cómo evitar las estafas mediante tarjetas magnéticas?", Periódico Granma, 13 de agosto de 2021. Disponible en: https://www.granma.cu/cuba/2021-08-13/como-evitar-las-estafas-mediante-tarjetas-magneticas-10-08-2021-20-08-11

González Rus, Juan José, "Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos", Revista de la Facultad de Derecho de la Universidad Complutense, ISSN 0210-1076, Número Extra 12, 1986.

Gorostidi, Jon López, ·Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia", Revista chilena de Derecho y Tecnología, Volumen 11, No 1, Santiago de Chile, junio 2022. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842022000100121&lng=es&nrm=iso

Gutiérrez Francés, María Luz, "Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual" Revista electrónica del Departamento de Derecho de la Universidad de La Rioja (REDUR) Número 3, 2005.

Hernández Díaz, Leyre, "El Delito Informático", Revista Eguzkilore: Cuaderno del Instituto Vasco de Criminología, Número 23, San Sebastián, diciembre 2009. Disponible en: https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Herrera Gandol, Dimas Alfredo. Conductas definidas como delitos informáticos o ciberdelitos en la legislación nacional y el derecho comparado, 2020. Disponible en: https://www.fgr.gob.cu/en/node/6954

Hikal, Wael, "Los Factores criminógenos exógenos", Revista de l'Institut Universitari d'Investigació en Criminologia i Ciències Penals de la Universidad de Valencia, 2009. Disponible en: https://www.uv.es/iccp/recrim/recrim09/recrim09n07.pdf

Hikal-Carreón, Wael Sarwat, "La especialización de la criminología: De lo general a lo específico, ¿hacía una neocriminología? teoría de las criminologías específicas", Revista Derecho y Cambio Social, Volumen 10, Número 32, 2013.

Jaishankar, Karuppannan, "Cyber criminology: Evolving a novel discipline with a new journal International", Journal of Cyber Criminology, 2007.

Jamidulin, Airat. Ciberdelincuencia: un instrumento de injerencia en los asuntos internos de los Estados, Periódico Juventud Rebelde, 11 de julio del 2019. Disponible en: https://www.juventudrebelde.cu/ciencia-tecnica/2019-07-10/ciberdelincuencia-un-instrumento-de-injerencia-en-los-asuntos-internos-de-los-estados

Jiménez Rozas, Jéssica, CIBERDELINCUENCIA: Evolución y relación con la actual situación de pandemia. Nuevas modalidades y nuevas problemáticas, Trabajo fin de grado curso de adaptación al grado en Criminología, junio del 2022. Disponible en: https://gredos.usal.es/bitstream/handle/10366/150144/TG_Jim%C3%A9nezRozas_Ciberdelincuencia.pdf?sequence=1&isAllowed=y

Kigerl, Alex, "Interrumpir el proceso de aparición de la ciberdelincuencia: de los delincuentes motivados a los ciberataques", 6to Informe Internacional Prevención de la criminalidad y seguridad cotidiana: Prevenir la ciberdelincuencia, Montreal, 2018. Disponible en: https://cipc-icpc.org/es/informe/informes-internacionales/6o-informe-internacional-sobre-la-prevencion-de-la-criminalidad-y-la-seguridad-cotidiana-prevenir-la-ciberdelincuencia/

Koops, Bert-Jaap, "The internet and its opportunities for cybercrime, Transnational Criminology", Manual I, 2010.

Lamperti, Sabrina, Problemáticas en torno a la investigación de los delitos informáticos, Universidad Fasta Federación Iberoamericana de Asociaciones de Derecho e Informática. Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática, Mar del Plata, 2014, Disponible en: https://www.researchgate.net/publication/324064192_Problematicas_en_torno_a_la_Investigacion_de_delitos_informaticos.

Littlejohn Shinder, Debra, Prevención y detección de delitos informáticos, Editorial Anaya, 1era edición, Madrid, 2003

Llano Pereira, Irma, El Desafío de la Cooperación Internacional, el cibercrimen y la justicia penal en el ciberespacio, Seminario de la Unión Europea y del Consejo de Europa con las regiones de América Latina y el Caribe, Paraguay, 2020. Disponible en: https://rm.coe.int/cibercrimen-y-la-justicia-penal-en-el-ciberespacio-irma/16809f0321

Mata y Martín, Ricardo Manuel, "Criminalidad informática: una introducción al cibercrimen" en Revista Actualidad Penal, Número 36, 2003.

Mata y Martín, Ricardo, Delincuencia informática y Derecho Penal, Editorial Hispamer, Nicaragua, 2003.

Mayer Lux, Laura, "El bien jurídico protegido en los delitos informáticos", Revista chilena de Derecho, Volúmen 44, Número 1, 2018. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-34372017000100011

Medina Gómez, Diana, "Los delitos cibernéticos y los problemas a enfrentar", Revista jurídica de la UNAM, 2020. Disponible en: https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543

Miró Llinares, Fernando, "Crimen, cibercrimen y COVID-19. Desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos", Revista de Internet, derecho y política, Número 32, 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7962061

Miró Llinares, Fernando, "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", Revista Electrónica de Ciencia Penal y Criminología, Número 13, 2011. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4396388, consultado el 11/4/2023, a las 20.00

Miró Llinares, Fernando, Delincuencia asociada al uso de las TIC, Universitat Oberta de Catalunya. Disponible en: http://cv.uoc.edu/annotation/49e137c73e26ddcd8cd71e5e8e4b66cd/803643/PID_00195946/PID_00195946.html

Miró Llinares, Fernando, El cibercrimen, Fenomenología y criminología de la delincuencia en el ciberespacio, Ediciones Jurídicas y Sociales. S.A, Marcial Pons, Madrid, 2012.

Mora, Endira; Yoselin Sánchez; Oscar, González y Daniel, Quintero, "Los Delitos Informáticos: Experiencia Investigativa en CENDITEL", Revista Conocimiento Libre y Licenciamiento, Número 16, 2017. Disponible el: https://convite.cenditel.gob.ve/revistaclic/index.php/revistaclic/article/view/908

Morales Delgado, Deivid Yuly, La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Universidad Señor de Sipán, Perú, 2015. Disponible en: https://repositorio.uss.edu.pe/handle/20.500.12802/3161

Ortiz Pradillo, Juan Carlos, "Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica" en El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito, Pérez Gil, Julio (Coord), Editorial La Ley, Madrid, 2012.

Ortiz Pradillo, Juan Carlos, La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación, Fundación Alternativas, Madrid, 2013.

Patiño Ortega, María, "Teoría de la elección racional de Cornish y Clarke", Revista Crimipedia, Revista editada en Elche por el Centro Crímina para el Estudio y Prevención de la Delincuencia, 2016. Disponible en: https://crimipedia.umh.es/topics/teoria-de-la-eleccion-racional-de-cornish-y-clarke/

Periódico Granma, "Wifi falsas y robo de cuentas Nauta en zonas públicas de acceso a internet en Cuba", 27 de diciembre del 2017. Disponible en: https://www.escambray.cu/2017/wifi-falsas-y-robo-de-cuentas-nauta-en-zonas-publicas-de-acceso-a-internet-en-cuba/

Puig Meneses, Yaima, De la informatización de la sociedad a la transformación digital en Cuba, 13 de diciembre de 2021. Disponible en: https://www.presidencia.gob.cu/es/noticias/de-la-informatizacion-de-la-sociedad-a-la-transformacion-digital-en-cuba/

Restrepo, Hugo Armando, Comercio electrónico: Importancia de la ciberseguridad en las transacciones electrónicas realizadas en las plataformas de compra online y en redes sociales en Colombia, Trabajo de

grado presentado como requisito para optar al título de Ingeniero de sistemas. Universidad Nacional Abierta y a Distancia UNAD, marzo 2023.

Rincón Ríos, Jarvey, El delito en la cibersociedad y la justicia penal internacional, Tesis Doctoral para optar al grado de Doctor, Madrid, 2015. Disponible en: https://eprints.ucm.es/33360/

Rodríguez Gómez, Nuria, "Teoría de la Oportunidad Diferencial de Richard A. Cloward y Lloyd E. Ohlin", Revista CRIMIPEDIA, Editada en Elche por el Centro Crímina para el Estudio y Prevención de la Delincuencia, Alicante, España, 2015.

Rojo Ramos, Jorge; Carlos, Ferrera-Granados; Carlos Mañanas Iglesias; y Juan Carlos, Guevara Pérez, "Estudio descriptivo de Cibervictimización en una muestra de estudiantes de Educación Secundaria Obligatoria", Revista Electrónica Interuniversitaria de Formación del Profesorado, Volumen 25, número 1, 2022. Disponible en: https://dialnet.unirioja.es/descarga/articulo/8272669.pdf

Romeo Casabona, Carlos María e Iñigo de Miguel, Beriain, El cibercrimen económico y patrimonial. Guía Docente, Departamento de Derecho Público y Cátedra Interuniversitaria, Diputación Foral de Bizkaia, de Derecho y Genoma Humano, Universidad del País Vasco. Disponible en: https://ocw.ehu.eus/mod/resource/view.php?id=32682

Romeo Casabona, Carlos María y Miguel, Beriain, El cibercrimen en el ámbito económico y patrimonial, Universidad del País Basco, Euskal Herriko Unibersitatea. Disponible en: https://ocw.ehu.eus/mod/resource/view.php?id=32683

Romeo Casabona, Carlos María, "Delitos Informáticos de carácter patrimonial", Revista Informática y Derecho, Universidad de La Laguna, 1996. Disponible en: https://dialnet.unirioja.es/descarga/articulo/248763.pdf

Salomon Clotet, Juan, "Delito informático y su investigación", Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?, Cuadernos de derecho judicial, Número 3, 2006.

Sánchez Vera, Fulgencio; Javier Eloy, Martínez Guirao; y Anastasia, Téllez Infantes, "La seguridad en el ciberespacio desde una perspectiva sociocultural", Methaodos, Revista de Ciencias Sociales, 2022, Volumen 10, Número 2, p.244. Disponible en: https://doi.org/10.17502/mrcs.v10i2.577

Serrano Santoyo Arturo y Evelio, Martinez Martínez, La Brecha Digital: Mitos y Realidades, Editorial UABC, México, 2003.

Superintendencia de institutos de formación profesional del Ministerio de Seguridad, Cibercrimen Y Delitos Informaticos. Apuntes para la materia, Buenos Aires, 2022. Disponible en: https://www.mseg.gba.gov.ar/areas/Vucetich/MANUALES%20DE%20MATERIAS%202022/MANUAL%20Cibercrimen%20y%20delitos%20inform%C3%A1ticos.pdf

Tamarit Sumalla, Josep, "Ciberdelincuencia y victimización", Revista de Internet Derecho y Política, Número 22, 2016. Disponible en: http://journals.uoc.edu/index.php/idp/article/view/n22-tamarit/n22-tamarit-pdf-es>http://dx.doi.org/10.7238/idp.v0i22.2991>

Temperini, Marcelo GI, "Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado en XLIII Jornadas Argentinas de Informática e Investigación Operativa", XIV

Simposio Argentino de Informática y Derecho, Buenos Aires, 2014. Disponible en: http://sedici.unlp.edu.ar/handle/10915/42145

Ugarte Almeida, Tamara Johanna, Acosta Ramírez, Nadia y Soto Medina, Lanny Sofía, "La delincuencia informática", Revista Caribeña de Ciencias Sociales, octubre 201. Disponible en: https://www.eumed.net/rev/caribe/2015/10/delincuencia-informatica.html

Violat Avila, Marta. El porqué de la ciberdelincuencia, 2020. Disponible en: https://derechodelared.com/el-porque-de-la-ciberdelincuencia/

Wall, David, Cybercrime: The Transformation of Crime in the Information Age, 2nd edition, Cambridge, Cambridge: Polity, 2024. Disponible en: https://www.wiley.com/enus/Cybercrime%3A+The+Transformation+of+Crime+in+the+Information+Age-p-9780745653532

Instrumentos Legales Internacionales

Boletín Oficial Del Estado Español, BOE, "Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia", hecho en Budapest el 23 de noviembre de 2001, No. 226, de 17 de septiembre de 2010, páginas 78847 a 78896 (50 págs.) Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

Centro Internacional para la prevención de la criminalidad, Informe Internacional. Prevención de la criminalidad y seguridad cotidiana: Prevenir la ciberdelincuencia, 2018. Disponible en: https://cipc-icpc.org/es/informe/informes-internacionales/6o-informe-internacional-sobre-la-prevencion-de-la-criminalidad-y-la-seguridad-cotidiana-prevenir-la-ciberdelincuencia/

Conferencia de ministros de justicia de los países iberoamericanos, Secretaría General, Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia, 28 de mayo del 2014. Disponible en: https://ficp.es/wp-content/uploads/CONVENIO-CIBERDELITO-VERSION-A-LA-FIRMA.pdf

Conferencia de ministros de justicia de los países iberoamericanos, Secretaría General, Recomendación Relativa a la Tipificación y Sanción de la Ciberdelincuencia, 28 de mayo del 2014. Disponible en: https://ficp.es/wp-content/uploads/Recomendacion-Ciber-VERSI%C3%93N-A-LA-FIRMA.pdf

Cubadebate, "Cuba contra el delito: Detenidos autores de defraudaciones en plataformas de pago digitales". Disponibles en: http://www.cubadebate.cu/noticias/2022/01/31/contra-el-delito-detenidos-autores-de-defraudaciones-en-plataformas-de-pago-digitales

Secretaría de Naciones Unidas, Enfoques amplios y equilibrados para prevenir y afrontar adecuadamente formas nuevas y emergentes de delincuencia transnacional, 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Doha, 12 a 19 de abril de 2015. Disponible en: https://www.unodc.org/documents/congress/Documentation/A-CONF.222-8/ACONF222_8_s_V1500541.pdf.

Instrumentos legales Nacionales

Asamblea Nacional del Poder Popular, Ley 151/2022 "Código Penal". Gaceta Oficial No. 93 Ordinaria de 1ro. de septiembre de 2022, República de Cuba, Ministerio de Justicia.

Consejo de Estado, Decreto-Ley No. 370/2018 "Sobre la Informatización de la Sociedad en Cuba". Consejo de Estado Gaceta Oficial No. 45 Ordinaria del 4 de julio del 2029, República de Cuba, Ministerio de Justicia.

Consejo de Ministros, Decreto No. 360/2019 "Sobre la Seguridad de la Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional", Gaceta Oficial No. 45 Ordinaria del 4 de julio del 2029, República de Cuba, Ministerio de Justicia.

Consejo de Estado, Decreto-Ley No. 35/2021 "De las telecomunicaciones, las tecnologías de la Información y la Comunicación y el uso del espectro radioeléctrico", Gaceta Oficial No. 92 Ordinaria del 17 de agosto del 2021, República de Cuba, Ministerio de Justicia.

Consejo de Ministros, Decreto 42/2021 "Reglamento General de Telecomunicaciones y las tecnologías de la Información y las Comunicaciones", Gaceta Oficial No. 92 Ordinaria del 17 de agosto del 2021, República de Cuba, Ministerio de Justicia.

Consejo de Ministros, Decreto 43/2021 "Reglamento Sobre el Uso del Espectro Radioeléctrico", Gaceta Oficial No. 92 Ordinaria del 17 de agosto del 2021, República de Cuba, Ministerio de Justicia.

Ministerio de Comunicaciones, Resolución 105/2021 "Reglamento sobre el Modelo de Actuación Nacional para la respuesta a incidentes de Ciberseguridad", Gaceta Oficial No. 92 Ordinaria del 17 de agosto del 2021, República de Cuba, Ministerio de Justicia.

Ministerio de Comunicaciones, Resolución 107/2021 "Reglamento para el Uso de los Servicios de Radiocomunicaciones por Satélites", Gaceta Oficial No. 92 Ordinaria del 17 de agosto del 2021, República de Cuba, Ministerio de Justicia.

Ministerio de Comunicaciones, Resolución 108/2021 "Reglamento para el Uso de los Servicios de Radiocomunicaciones por Satélites", Gaceta Oficial No. 92 Ordinaria del 17 de agosto del 2021, República de Cuba, Ministerio de Justicia.